David Kirby

ECE 529: Introduction to Technical Cybersecurity

Spring, 2022

# Campaign Design

This assignment has two parts[1] — first we have been tasked with designing a campaign that will attack a system (your system) to seek out any available exploits; then, using our new-found knowledge of the system's vulnerabilities, we must turn around and defend the system from similar attacks. The system in this case is an increasingly vulnerable target, an older IoT device: a TP-Link NC200 cloud camera. We must design the campaign architecture, discover a potential attack surface, define the attack vectors of the attack surface, and finally, find available exploits for these attack vectors. Once we have rooted out possible exploits, we will offer suggestions on how to defend the camera from further malicious actors.

As discussed in the lecture videos, there are four different types of campaigns — criminal campaigns, for which the primary goal is of course money; nation states that are usually focused on information or sabotage; organizations, which can run the full gamut of malicious intents; and then basic hobbyists, people that are simply interested in cybersecurity and malware. The purpose of our attack on the TP-Link is purely from a hobbyist standpoint. This assignment is an exploratory analysis, similar, I imagine, to one a company might hire a third-party consulting firm to run in an effort to detect vulnerabilities in their system.

---

https://learn.unm.edu/webapps/assignment/uploadAssignment?content_id=_7770458_1&course_id=_110809_1

Each of these campaigns have a specific kind of architecture, they have particular goals they want to accomplish, strategies (big pictures for how they intend to go about reaching those goals), and principles (rules of engagement). Once we have established the why, we need to lay out the how. To do this we will need to determine the assets we have available, the skillsets we can tap into, and the openness of the internet access to the target. We will need to look at the tools available to use. Finally, we will need to look at what tactics we are willing to use and what information do we have with respect to this particular target.

For this campaign, we are mostly focused on intelligence operations, gathering information. Our end goal is not entirely clear, perhaps extortion, but mostly fun. We know we have a potential asset with the TP-Link camera. We are not trying to get expelled in our last semester of graduate school, so our principles are relatively benign (no phishing attacks because those are almost always successful). We will investigate potential attack surfaces and attack vectors that will allow us to access the cloud camera, then using various known exploits, attempt to penetrate the target.

Now that we have ascertained what type of campaign we will be carrying out, we need to determine an attack surface. The example that we will use is Mirai, a type of malware[2] that primarily uses default credentials to log on to devices, a significant problem in the industry. It scans networks for certain types of IoT devices and turns them into bots. This is an ever-expanding problem especially

[2] https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/

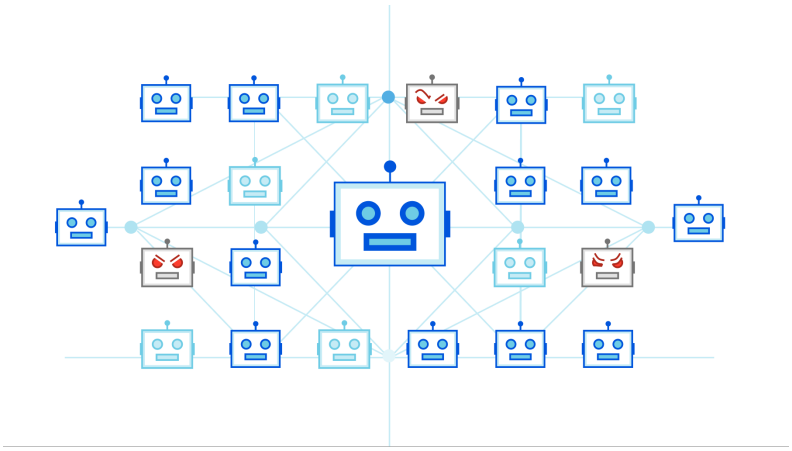

**FIGURE 1: BOTNETS INFECT SUSCEPTIBLE HOSTS.**

given how many devices ship with older embedded operating systems that do not have adequate security (as we will see with the TP-Link NC200).

While performing reconnaissance on the TP-Link NC200, we found that on older firmware (<= 2.1.9 build 200225), a hardcoded encryption key is used to encrypt/decrypt configuration backup files[3]. We could exploit this vulnerability to decrypt backup[4] files and get access to:

- Alarm FTP server user and password
- WLAN passphrase
- PPPoE user and password
- Alarm SMTP server user and password
- DDNS user and password

Using these passwords, we could disrupt the entire network, change the Wi-Fi SSID, use the SMTP server to spam, use the PPPoE credentials to create havoc with your ISP, and any number of nefarious deeds.

[3] https://nvd.nist.gov/vuln/detail/CVE-2020-12110

[4] https://seclists.org/fulldisclosure/2020/May/3

We could also create a false encrypted backup that would be used to restore the camera. This would allow us to inject malicious files and execute them with root privileges (including setting up a botnet like Mirai). Additionally, we found that the camera streams to a cloud service hosted by TP-Link, which has an internet-facing portal for viewing remotely[5]. We could use this, along with the credentials we obtained, to create an RTSP feed and broadcast it anywhere. With this feed, the camera LED would not even be on, and no one would ever know.

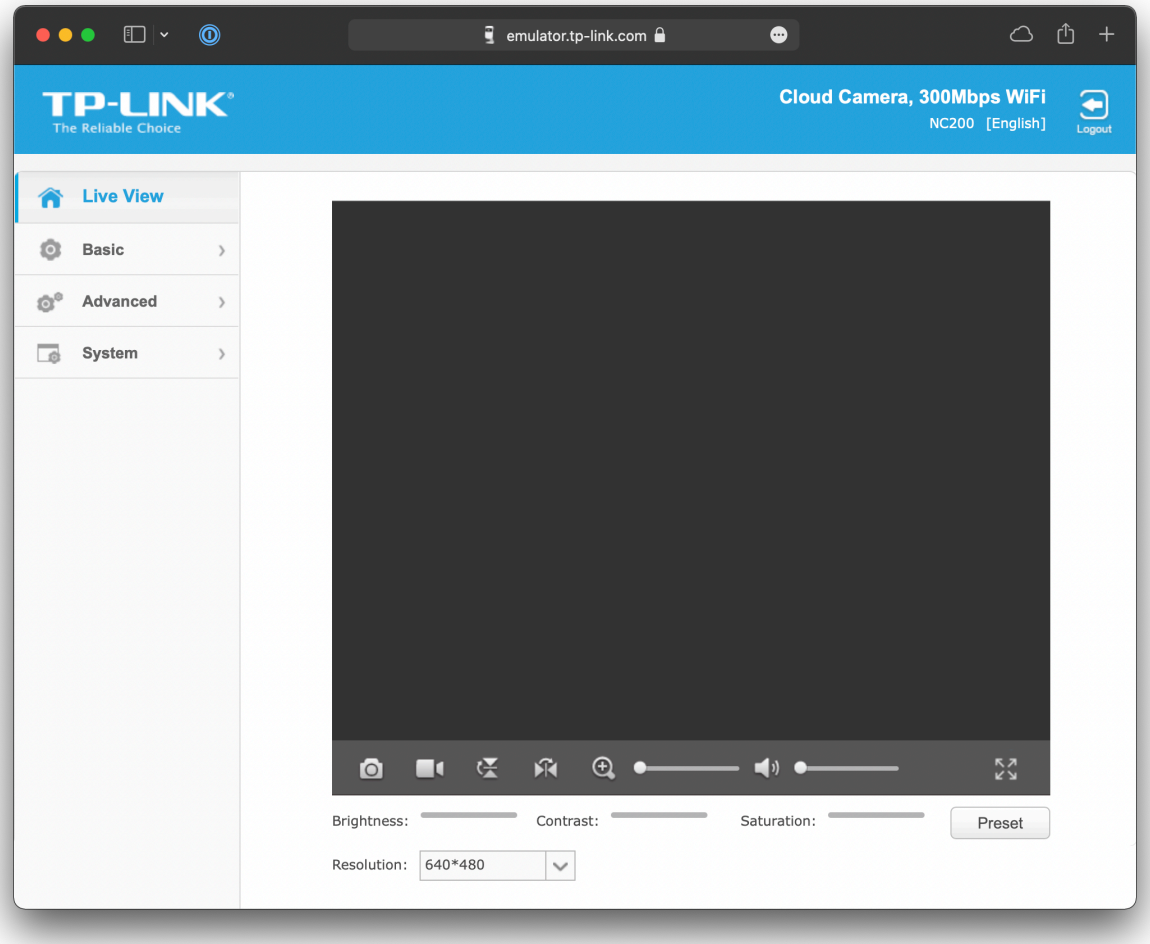


**FIGURE 2: TP-LINK EMULATOR SHOWING REMOTE WEB INTERFACE.**

[5] https://www.tp-link.com/us/support/download/tl-nc200/#Emulators

Further, the TP-Link NC200 doubles as network router, enabling us to potentially pivot to other systems connected to the target. This creates an attack graph that goes well beyond just the scope of this assignment and puts the professor's entire network in jeopardy.

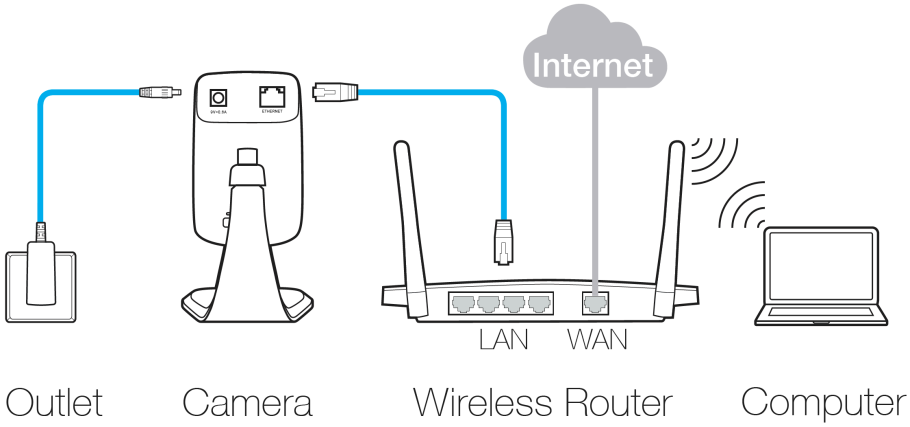


**FIGURE 3: ATTACK GRAPH CONTAINS ENTIRE NETWORK.**

In addition to the hardcoded encryption key vulnerability, there appears to be an exploit published on NIST6 where an attacker could send a login request without a user-agent HTTP header and crash the process that handles the IP camera. This could easily be done using curl and manually setting the user-agent: `curl -H "User-Agent:" example.com`. Once the process has been compromised, we could use default credentials to bypass the credentials requirement[7].

Given the severity of these exploits, let us now turn to how we could secure the target. Analyzing the different attack surfaces, we see that the most significant among them are the hardcoded encryption key and the NULL user-

[6] https://nvd.nist.gov/vuln/detail/CVE-2020-10231

[7] https://seclists.org/fulldisclosure/2020/Apr/5

agent. If we can secure those, then we can mitigate a majority of the other threats. As the professor pointed out in the videos for this module, keeping firmware and software updated is paramount and helps to thwart most malicious actors. As such, from the reconnaissance, we found that TP-Link has released updated firmware that addresses both of these vulnerabilities. It is our recommendation that the professor immediately update and consider turning on automatic updates if not already on. This is good advice for any IoT device and any internet-connected device in general. This assignment persuaded me to check my own IoT devices for known exploits and to check for firmware updates. Other general tips recommended for securing a home network include: changing default credentials on devices, but especially routers as they are the main gatekeepers to your entire network; creating secure wireless passwords, preferably with a password manager; enabling WPA2/WPA3 wireless encryption on your router; disabling WPS; disabling UPnP; disabling router web access via WAN; disabling ping via WAN; disabling DMZ; and disabling port trigger and port forwarding. Also practicing due diligence when clicking on links and opening files from unknown sources. These could all help to reduce the risk of malicious attacks.